(13) (10)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-339080
(43)Date of publication of application : 10.12.1999

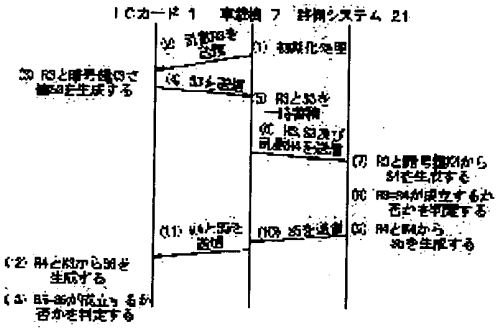
(51)Int.Cl. G07B 15/00
G07B 15/00
G06K 17/00

(21)Application number : 10-148074
(22)Date of filing : 28.05.1998

(71)Applicant : MITSUBISHI HEAVY IND LTD
(72)Inventor : KATO MASAKI

(54) SECURITY DEVICE OF TOLL COLLECTION DEVICE FOR TOLL ROAD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security device of the toll collection device for a toll road which can effectively prevent a cipher key group from being exposed.
SOLUTION: A moving-body-side controller is equipped with an IC card 1 and an on-vehicle machine 7 where the IC card is inserted and extracted. Here, the iC card 1 is stored with data representing a moving-body-side cipher key group K3 and a road-side controller 21 is stored with data representing a road-side cipher key group K4; and at least one of the road-side controller 2 and moving-body-side controller decides whether or not the moving-body-side cipher key group K3 and road-side cipher key group K4 match each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－339080

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｂ　15/00		Ｇ０７Ｂ　15/00	Ｌ
	５１０		５１０
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
			Ｌ

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平10－148074

(22)出願日　平成10年(1998)５月28日

(71)出願人　000006208
三菱重工業株式会社
東京都千代田区丸の内二丁目５番１号

(72)発明者　加藤　聖樹
兵庫県神戸市兵庫区和田崎町一丁目１番１号　三菱重工業株式会社神戸造船所内

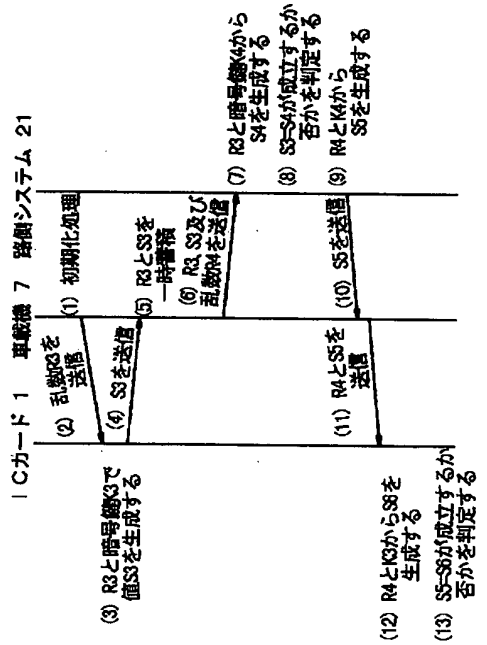
(74)代理人　弁理士　工藤　実　（外１名）

(54)【発明の名称】　有料道路の料金収受装置におけるセキュリティ装置

(57)【要約】

【課題】　暗号鍵群の暴露を有効に防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供する

【解決手段】　移動体側制御装置７Ａは、ＩＣカード１と、前記ＩＣカードが挿脱される車載機７とを備え、前記ＩＣカードに移動体側暗号鍵群Ｋ３を示すデータが格納され、道路側制御装置２１に道路側暗号鍵群Ｋ４を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定する。



001.gif

1

【特許請求の範囲】

【請求項１】　相互に通信可能な道路側制御装置（２１）および移動体側制御装置（７Ａ）とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、

前記移動体側制御装置（７Ａ）は、

ＩＣカード（１）と、

前記ＩＣカード（１）が挿脱される車載機（７）とを備え、

前記ＩＣカード（１）に移動体側暗号鍵群（Ｋ３）を示すデータが格納され、

前記道路側制御装置（２１）に道路側暗号鍵群（Ｋ４）を示すデータが格納され、

前記道路側制御装置（２１）および前記移動体側制御装置（７Ａ）の少なくとも一方は、前記移動体側暗号鍵群（Ｋ３）と前記道路側暗号鍵群（Ｋ４）が一致しているか否かを判定する（ステップＳ８，ステップＳ１３）

有料道路の料金収受装置におけるセキュリティ装置。

【請求項２】　請求項１記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側制御装置（７Ａ）は、

暗号化情報（Ｒ３，Ｒ４）を発生する暗号化情報発生手段と、

前記暗号化情報発生手段が発生した前記暗号化情報（Ｒ３）を示すデータおよび前記移動体側暗号鍵群（Ｋ３）を示すデータを用いて第１の生成情報（Ｓ３）を生成する（ステップＳ３）ための移動体側演算処理手段（２）とを備えてなり、

前記道路側制御装置（２１）は、

前記移動体側制御装置（７Ａ）と通信して入手した前記暗号化情報（Ｒ３）を示すデータ、および前記道路側暗号鍵群（Ｋ４）を示すデータを用いて第２の生成情報（Ｓ４）を生成する（ステップＳ７）ための道路側演算処理手段を備えてなり、

前記道路側制御装置（２１）および前記移動体側制御装置（７Ａ）の少なくとも一方は、前記移動体側暗号鍵群（Ｋ３）と前記道路側暗号鍵群（Ｋ４）が一致しているか否かを判定するときに、前記第１の生成情報（Ｓ３）を示すデータと前記第２の生成情報（Ｓ４）を示すデータとが一致しているか否かを判定する（ステップＳ８）

有料道路の料金収受装置におけるセキュリティ装置。

【請求項３】　請求項１記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側制御装置（７Ａ）は、

暗号化情報（Ｒ３，Ｒ４）を発生する暗号化情報発生手段と、

移動体側演算処理手段（２）とを備えてなり、

前記道路側制御装置（２１）は、道路側演算処理手段を備えてなり、

前記移動体側制御装置（７Ａ）は、

2

前記暗号化情報発生手段により発生させた第１の前記暗号化情報（Ｒ３，ステップＳ２）を示すデータと、

前記第１の暗号化情報（Ｒ３）を示すデータと前記移動体側暗号鍵群（Ｋ３）を示すデータとを用いて前記移動体側演算処理手段（２）により生成させた第１の生成情報（Ｓ３，ステップＳ３）を示すデータと、

前記暗号化情報発生手段により発生させた第２の前記暗号化情報（Ｒ４）を示すデータと、を前記道路側制御装置（２１）に送信し（ステップＳ６）、

前記道路側制御装置（２１）は、前記第１の暗号化情報（Ｒ３）を示すデータと前記道路側暗号鍵群（Ｋ４）を示すデータとを用いて前記道路側演算処理手段により第２の生成情報（Ｓ４）を生成し（ステップＳ７）、

かつ、前記第１の生成情報（Ｓ３）と前記第２の生成情報（Ｓ４）とが一致しているか否かを判定して前記道路側暗号鍵群（Ｋ４）を示すデータと前記移動体側暗号鍵群（Ｋ３）を示すデータが一致しているか否かの第１の認証を行い（ステップＳ８）、

かつ、前記第２の暗号化情報（Ｒ４）を示すデータと前記道路側暗号鍵群（Ｋ４）を示すデータとを用いて前記道路側演算処理手段により第３の生成情報（Ｓ５）を生成し（ステップＳ９）、

かつ、前記第３の生成情報（Ｓ５）を示すデータを前記移動体側制御装置（７Ａ）に送信し（ステップＳ１０）、

前記移動体側制御装置（７Ａ）は、前記第２の暗号化情報（Ｒ４）を示すデータと前記移動体側暗号鍵群（Ｋ３）を示すデータとを用いて前記移動体側演算処理手段（２）により第４の生成情報（Ｓ６）を生成し（ステップＳ１２）、

かつ、前記第４の生成情報（Ｓ６）と前記第３の生成情報（Ｓ５）とが一致しているか否かを判定して、前記移動体側暗号鍵群（Ｋ３）を示すデータと前記道路側暗号鍵群（Ｋ４）を示すデータとが一致しているか否かの第２の認証を行う（ステップＳ１３）有料道路の料金収受装置におけるセキュリティ装置。

【請求項４】　請求項１から３のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側暗号鍵群（Ｋ３）を示すデータは、前記移動体側制御装置（７Ａ）のうち前記ＩＣカード（１）にのみ格納されている有料道路の料金収受装置におけるセキュリティ装置。

【請求項５】　請求項２から４のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側演算処理手段（２）は、前記ＩＣカード（１）に備えられている有料道路の料金収受装置におけるセキュリティ装置。

【請求項６】　請求項３から５のいずれかに記載の有料

道路の料金収受装置におけるセキュリティ装置において、

前記第２の認証は、前記ＩＣカード（１）で行われる有料道路の料金収受装置におけるセキュリティ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、有料道路の料金収受装置におけるセキュリティ装置に関する。

【０００２】

【従来の技術】有料道路では、料金収受がゲートで行われる。各自動車は、料金収受のために減速しゲートで停止し、料金収受の後に再び加速する。このような加減速は、交通渋滞を招くだけでなく、燃料消費量と廃棄ガス量を増大させる。このような加減速を不要とするために、料金収受をノンストップで行う試みがなされている。

【０００３】これは、無線通信機能を持つ車載機を車両に搭載し、この車載機と、料金所に装備された路上機アンテナとの間で、料金収受を行うものである。図３を参照して、上記料金収受システムの一例を説明する。

【０００４】図３に示すように、料金収受システムは、道路側制御システム６８と、移動体側制御システム５３Ａとを備えている。道路側制御システム６８は、第１のアンテナ５８と、第１のアンテナコントローラ５９と、第２のアンテナ６０と、第２のアンテナコントローラ６１と、車両検知センサ６２と、車両検知センサコントローラ６３と、不正防止カメラ６４と、不正防止カメラコントローラ６５と、これらのコントローラ５９，６１，６３，６５を統括してコントロールする道路側コントローラ６６とを備えている。道路側制御システム６８は、公衆回線または専用回線にて中央制御システム６７に接続されている。

【０００５】移動体側制御システム５３Ａは、車載機５３と、ＩＣカード５０とを備えている。ＩＣカード５０は、メモリ５２と、ＣＰＵ５１とを備えている。車載機５３は、ＩＣカードスロット５６と、ＣＰＵ５５と、ＲＦユニット５４と、メモリ５７とを備えている。車載機５３は、さらに表示ディスプレイ、ボタン、ＬＥＤ表示器等のヒューマンＩ／Ｆ（図示せず）を備えている。

【０００６】車載機５３のメモリ５７およびＩＣカード５０のメモリ５２には、それぞれ、所定の暗号鍵または暗号鍵群（以下、単に暗号鍵群と記す）が格納されている。

【０００７】次に、上記料金収受システムにおけるセキュリティシステムについて説明する。ここで、セキュリティシステムとは、ＩＣカード５０、車載機５３および道路側システム６８の偽造を防止するために、相互に認証を行うシステムをいう。上記のセキュリティシステムでは、車載機５３のメモリ５７に格納された暗号鍵群（「Ｋ２」とする）と、ＩＣカード５０のメモリ５２に格納された暗号鍵群（「Ｋ１」とする）との一致が、車載機５３とＩＣカード５０との双方で認証される。

【０００８】このような暗号鍵群Ｋ１，Ｋ２の一致の相互認証の結果は、車載機５３から第１のアンテナ５８に送信される。相互認証が成立すれば、料金収受の手続きが道路側制御システム６８と移動体側制御システム５３Ａとの間で行われる。相互認証が成立しなかった場合は、不正防止カメラ６４により、その当該車載機５３を搭載した車を不正車として撮影するようになっている。なお、車両検知センサ６２は、相互認証が成立しない場合に、当該車両の通過を検知して不正防止カメラ６４を起動するためのものである。

【０００９】次に、図４を参照して、上記セキュリティシステムにおける相互認証の手順を、（１）から（１０）のステップに分けて説明する。

【００１０】（１）まず、車載機５３は、ＩＣカード５０がＩＣカードスロット５６に挿入された時点で、ＩＣカード５０に乱数Ｒ１を送信する。

（２）ＩＣカード５０は、その乱数Ｒ１とメモリ５２に格納された暗号鍵群Ｋ１で、値Ｓ１を作成する。数式表現では以下のようになる。

Ｓ１＝ｆ（Ｒ１、Ｋ１）……（式１）。

【００１１】（３）ＩＣカード５０は、値Ｓ１を車載機５３に送り返す。

（４）車載機５３は、乱数Ｒ１とメモリ５７に格納された暗号鍵群Ｋ２を使用して、式（１）と同じ計算を行い、値Ｓ２を求める。数式表現では以下のようになる。

Ｓ２＝ｆ（Ｒ１、Ｋ２）……（式２）。

（５）この結果、ＩＣカード５０のメモリ５２に内蔵された暗号鍵群Ｋ１と、車載機５３のメモリ５７に内蔵された暗号鍵群Ｋ２が同じ値であれば、その結果、Ｓ１＝Ｓ２、となるはずである。したがって、車載機５３は、Ｓ１＝Ｓ２、が成立するか否かを判定し、これが一致した場合には、ＩＣカード５０が同じ暗号鍵群を共有する（Ｋ１＝Ｋ２）カードであるとして、ＩＣカード５０の正当性を確認することになる。

【００１２】（６）次に、ＩＣカード５０は、乱数Ｒ２を発生させて、車載機５３に送信する。

（７）車載機５３は、その乱数Ｒ２を使用して以下の計算を実行する。

Ｓ３＝ｆ（Ｒ２、Ｋ２）……（式３）。

（８）値Ｓ３は、車載機５３からＩＣカード５０に送信される。

【００１３】（９）ＩＣカード５０では、以下の計算を行い、値Ｓ４を求める。

Ｓ４＝ｆ（Ｒ２、Ｋ１）……（式４）。

（１０）ＩＣカード５０は、Ｓ３＝Ｓ４、が成立するか否かを判定し、値Ｓ３と値Ｓ４が等しい場合に限り、車載機５３を同じ暗号鍵群を共有する（Ｋ１＝Ｋ２）ものとして、車載機５３の正当性を確認する。

5

【００１４】上記（１）から（１０）のステップの結果として、ＩＣカード５０と車載機５３の相互認証が成立することになる。

【００１５】上記において、暗号化に使用される暗号鍵群Ｋ１，Ｋ２に含まれる暗号鍵の数は、１つでなくてもよく、複数使用することができる。いずれにしても、ＩＣカード５０および車載機５３の各々は、同一の暗号鍵または同一の暗号鍵群を共有する必要がある。

【００１６】

【発明が解決しようとする課題】ところで、上記のような料金収受システムでは、ＩＣカード５０および車載機５３の各々が同一の暗号鍵群Ｋ１，Ｋ２を共有している。したがって、仮に車載機５３が分解されてメモリ５７の暗号鍵群Ｋ２が解析された場合には、車載機５３自体の偽造が可能となるのみならず、同じ暗号鍵群を共有するＩＣカード５０の暗号鍵群Ｋ１も暴露されることになり、ＩＣカード５０の偽造も可能になってしまうという問題がある。このような偽造を防止することが要請されている。

【００１７】本発明は、このような技術的背景に基づいてなされたものであり、次のような課題を解決するものである。本発明の目的は、暗号鍵群の暴露を防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供することにある。本発明の他の目的は、ＩＣカードまたは車載機の偽造を防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供することにある。本発明の更に他の目的は、数量が限定されセキュリティの管理が容易な有料道路の料金収受装置におけるセキュリティ装置を提供することにある。

【００１８】

【課題を解決するための手段】本発明の有料道路の料金収受装置におけるセキュリティ装置は、相互に通信可能な道路側制御装置および移動体側制御装置とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、前記移動体側制御装置は、ＩＣカードと、前記ＩＣカードが挿脱される車載機とを備え、前記ＩＣカードに移動体側暗号鍵群を示すデータが格納され、前記道路側制御装置に道路側暗号鍵群を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定する。

【００１９】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項１記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側制御装置は、暗号化情報を発生する暗号化情報発生手段と、前記暗号化情報発生手段が発生した前記暗号化情報を示すデータおよび前記移動体側暗号鍵群を示すデータを用いて第１の生成情報を生成するための移動体側演算処理手段とを備えてなり、前記道路側制御装置は、前記移動体側制御装置と通信して入手した前記暗号化情報

6

を示すデータ、および前記道路側暗号鍵群を示すデータを用いて第２の生成情報を生成するための道路側演算処理手段を備えてなり、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定するときに、前記第１の生成情報を示すデータと前記第２の生成情報を示すデータとが一致しているか否かを判定する。

【００２０】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項１記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側制御装置は、暗号化情報を発生する暗号化情報発生手段と、移動体側演算処理手段とを備えてなり、前記道路側制御装置は、道路側演算処理手段を備えてなり、前記移動体側制御装置は、前記暗号化情報発生手段により発生させた第１の前記暗号化情報を示すデータと、前記第１の暗号化情報を示すデータと前記移動体側暗号鍵群を示すデータとを用いて前記移動体側演算処理手段により生成させた第１の生成情報を示すデータと、前記暗号化情報発生手段により発生させた第２の前記暗号化情報を示すデータと、を前記道路側制御装置に送信し、前記道路側制御装置は、前記第１の暗号化情報を示すデータと前記道路側暗号鍵群を示すデータとを用いて前記道路側演算処理手段により第２の生成情報を生成し、かつ、前記第１の生成情報と前記第２の生成情報とが一致しているか否かを判定して前記道路側暗号鍵群を示すデータと前記移動体側暗号鍵群を示すデータが一致しているか否かの第１の認証を行い、かつ、前記第２の暗号化情報を示すデータと前記道路側暗号鍵群を示すデータとを用いて前記道路側演算処理手段により第３の生成情報を生成し、かつ、前記第３の生成情報を示すデータを前記移動体側制御装置に送信し、前記移動体側制御装置は、前記第２の暗号化情報を示すデータと前記移動体側暗号鍵群を示すデータとを用いて前記移動体側演算処理手段により第４の生成情報を生成し、かつ、前記第４の生成情報と前記第３の生成情報とが一致しているか否かを判定して、前記移動体側暗号鍵群を示すデータと前記道路側暗号鍵群を示すデータとが一致しているか否かの第２の認証を行う。

【００２１】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項１から３のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側暗号鍵群を示すデータは、前記移動体側制御装置のうち前記ＩＣカードにのみ格納されている。

【００２２】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項２から４のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側演算処理手段は、前記ＩＣカードに備えられている。

【００２３】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項３から５のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記第２の認証は、前記ＩＣカードで行われる。

【００２４】上記のように、ＩＣカードに秘密情報を集中し、ＩＣカードで論理演算を行うことにより、更に、ＩＣカードの偽造が困難になる。移動体側と固定側との間で必要十分条件を満たす相互の暗号同定化を行うためには、固定側の複雑な装置の中から秘密情報を盗む必要があるが、固定側装置の管理を厳格に行うことが可能であるから、暗号鍵群の暴露はほとんど不可能になる。ＩＣカードが盗まれた場合には、ただちに届け出を固定側装置の制御装置に対して行うことができるから、その偽造は実質的に不可能である。

【００２５】

【発明の実施の形態】以下、添付図面を参照して、本発明の有料道路の料金収受装置におけるセキュリティ装置の一実施の形態を説明する。

【００２６】図１は、本実施形態の装置ブロック図である。図１に示すように、本セキュリティシステムは、道路側制御システム２１と、移動体側制御システム７Ａとを備えている。道路側制御システム２１は、第１のアンテナ９を備えている。第１のアンテナ９は、第１のアンテナコントローラ１０によりその送受信が制御されている。第１のアンテナコントローラ１０には、道路側第１のメモリ１１が設けられている。この道路側第１のメモリ１１は、道路側暗号鍵群Ｋ４を格納している。

【００２７】道路側制御システム２１は、さらに、第２のアンテナ１２を備えている。第２のアンテナ１２は、第２のアンテナコントローラ１３によりその送受信が制御されている。第２のアンテナコントローラ１３には、道路側第２のメモリ１４が設けられている。道路側第２のメモリ１４は、道路側第１のメモリ１１と同様に、道路側暗号鍵群Ｋ４を格納している。

【００２８】第１のアンテナ９と、第１のアンテナコントローラ１０と、道路側第１のメモリ１１は、第１道路側認証用ユニットを形成する。第２のアンテナ１２と、第２のアンテナコントローラ１３と、道路側第２のメモリ１４は、第２道路側認証用ユニットを形成する。このような第１道路側認証用ユニットと第２道路側認証用ユニットは、例えば、有料道路の上り線用と下り線用として、または、出口用と入口用として、近接位置にまたは離隔位置に配置される。

【００２９】道路側制御システム２１は、さらに、車両検知センサ１５、車両検知センサコントローラ１６、不正防止カメラ１７、不正防止カメラコントローラ１８およびこれら諸機器を統一してコントロールするための道路側コントローラ１９を備えている。道路側コントローラ１９は各ゲートにそれぞれ配置され、これら複数の道路側コントローラ１９は、全体として中央制御システム２０により群管理が行われる。例えば、後述するＩＣカード１の盗難時には、そのカード番号が中央制御システム２０を介して複数の道路側制御システム２１に伝達される。

【００３０】移動体側制御システム７Ａは、ＩＣカード１と車載機７とを備えている。ＩＣカード１は、ＣＰＵ２とメモリ３とを備えている。メモリ３は、移動体側暗号鍵群Ｋ３を記憶しこれが更新されない限り永久的に保存している。車載機７は、ＩＣカードスロット６、ＣＰＵ５およびＲＦユニット４を備えている。

【００３１】車載機７は、移動体側暗号鍵群Ｋ３を保存していない。ここで、「移動体側暗号鍵群Ｋ３を保存していない」という意味について説明する。移動体側暗号鍵群Ｋ３は、Ｎ個の移動体側暗号鍵群Ｋ３１……Ｋ３Ｎの群でよい。この場合、車載機７は、移動体側暗号鍵群Ｋ３１……Ｋ３Ｎのうちのどの１つも保有していないということである。群の要素が１つの場合にも、それは群または集合である、という。

【００３２】次に、図２を参照して、本実施形態のセキュリティシステムについて説明する。ＩＣカード１は、車載機７のＩＣカードスロット６に挿入される。この挿入により、ＩＣカード１と車載機７は、初期化が行われる（図２においてステップ（１）参照。なお、以下、ステップ（１）は「ステップＳ１」、ステップ（２）は「ステップＳ２」…と称する）。

【００３３】車載機７は、第１移動体側暗号化情報Ｒ３を発生させる。ここで、前記暗号化情報は、例えば、乱数である。第１移動体側暗号化情報Ｒ３は、ＩＣカード１のＣＰＵ２に送信される（ステップＳ２参照）。ＣＰＵ２は、メモリ３に格納された移動体側暗号鍵群Ｋ３と第１移動体側暗号化情報Ｒ３とを用いて、次に示される演算子計算を行って生成値Ｓ３を生成する（ステップＳ３参照）。

Ｓ３＝ｆ（Ｒ３、Ｋ３）……（式５）。

【００３４】次いで、ステップＳ４に示すように、ＩＣカード１は、値Ｓ３を車載機７に送り返す。第１移動体側暗号化情報Ｒ３と値Ｓ３は、車載機７に一時的に蓄積される（ステップＳ５参照）。これらの値は、本セキュリティシステムの動作完了後には、車載機７からは消去される。車載機７の破壊によりＩＣカード１の偽造に必要な情報が盗用されるのを未然に防止するためである（この意味については後述する）。

【００３５】車載機７が道路側制御システム２１との交信可能領域に入ると、車載機７と道路側制御システム２１との間で双方向にデータをやり取りするための無線通信が行われる。すなわち、ステップＳ６に示すように、車載機７は、前記蓄積されているデータ（第１移動体側暗号化情報Ｒ３および、ＩＣカード１で計算された生成値Ｓ３）と、車載機７で発生させる第２移動体側暗号化

情報Ｒ４を、第１のアンテナ９に送信する。これらの３つのデータＲ３，Ｓ３，Ｒ４は、第１のアンテナコントローラ１０に送られる。

【００３６】ステップＳ７に示すように、第１のアンテナコントローラ１０は、第１移動体側暗号化情報Ｒ３と、メモリ１１に格納されている道路側暗号鍵群Ｋ４とを使用して、式（１）と同形の演算子計算を行い生成値Ｓ４を求める。

Ｓ４＝ｆ（Ｒ３、Ｋ４）……（式６）。

【００３７】次いで、ステップＳ８に示すように、Ｓ３＝Ｓ４、の関係が成立するか否かを判定する。成立すると判定されれば、第１のアンテナコントローラ１０は、道路側第１のメモリ１１とＩＣカード１が、同一または共通の暗号鍵を共有する（Ｋ３＝Ｋ４）ものとして、両側システムの同定を確認して、ＩＣカード１の正当性を確認・認証してよいことになる。

【００３８】次に、ステップＳ９に示すように、第１のアンテナコントローラ１０は、第２移動体側暗号化情報Ｒ４と、道路側暗号鍵群Ｋ４を使用して、次の計算を行う。

Ｓ５＝ｆ（Ｒ４、Ｋ４）……（式７）。

【００３９】この生成値Ｓ５は、第１のアンテナ９を介して車載機７に送信される（ステップＳ１０）。次いで、ステップＳ１１に示すように、車載機７は、第２移動体側暗号化情報Ｒ４と生成値Ｓ５とをＩＣカード１に送信する。

【００４０】次に、ＩＣカード１は、次の計算を実行する（ステップＳ１２）。

Ｓ６＝ｆ（Ｒ４、Ｋ３）……（式８）

この結果、Ｓ５＝Ｓ６の関係が成立するか否かが判定され（ステップＳ１３）、成立していれば、ＩＣカード１は、道路側第１のメモリ１１とＩＣカード１が同一または共通の暗号鍵群を共有する（Ｋ３＝Ｋ４）ものとして、両側システムの同定を確認して、道路側制御システム２１の全体の正当性を確認・認証してよいことになる。この認証結果は、車載機７を介して第２のアンテナ１２に送信されることになる。

【００４１】上記のように、本実施形態では、ＩＣカード１と同一または共通の暗号鍵群を共有するものは、車載機７ではなく、道路側制御システム２１である。したがって、道路側制御システム２１を破壊等して暗号鍵群Ｋ４を解析しない限り、ＩＣカード１を持たない第三者にＩＣカード１の暗号鍵群Ｋ３が暴露されることはない。したがって、不特定多数存在し盗難等の管理を行い難い車載機７に、暗号鍵群Ｋ４を記憶させておく場合に比べて、本実施形態は、ＩＣカード１の偽造防止に有効である。

【００４２】すなわち、暗号鍵群Ｋ４が道路側制御システム２１に記憶されている以上、相互認証を行うに際しては、道路側制御システム２１が必須となる。このことから、ＩＣカード１が行う計算である式（８）（図２のステップＳ１２）についても、道路側制御システム２１自らが、ＩＣカード１と車載機７とを利用して計算したことに等価であるといえる。言い換えると、相互認証は、道路側制御システム２１により確認されたことになる。セキュリティの管理の観点から、道路側制御システム２１による確認は、従来の車載機による確認の場合に比べて、相互認証の精度も向上する。例えば、車載機は、道路側制御装置２１に比べて改造し易く、その場合、暗号鍵群が不一致の場合にも一致との認証を与えるように改造することも考えられる。これに対して、本実施形態の道路側制御装置２１の改造は、考えにくく、犯罪防止に有効である。

【００４３】第１のアンテナ９と第２のアンテナ１２の両方の使用により、駐車場の入口処理と出口処理とに分けることも可能である。既述の演算計算を含む処理の時間が十分にあれば、第１のアンテナ９だけで実行することが可能である。さらには、逆方向走行車両の処理を併行させることも可能である。

【００４４】以上に述べたように、本実施形態によれば、不特定多数に供給される車載機７ではなく、数量限定され、さらにセキュリティ面においても管理が容易な道路側制御システム２１内のアンテナコントローラ１０，１３だけに暗号鍵群Ｋ４を格納することにより、ＩＣカード１と共有された暗号鍵群Ｋ４の解読を困難にすることができ、ＩＣカードの偽造を未然に防止することができる。

【００４５】さらに、新規の暗号鍵群を有したＩＣカードが発行された場合でも、道路側制御システム内のメモリ１１、１４に格納された暗号鍵群を更新するのみでよく、不特定多数に供給された車載機７に格納された暗号鍵群を更新する場合と比較して、格段に容易にすることができる。さらにまた、車載機７は、暗号鍵群を安全に格納するメモリを有したり、暗号化のアルゴリズムを有する必要がないので、車載機７を非常に安価に構成することができるようになる。

【００４６】

【発明の効果】本発明による有料道路の料金収受装置におけるセキュリティ装置によれば、相互に通信可能な道路側制御装置および移動体側制御装置とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、前記移動体側制御装置は、ＩＣカードと、前記ＩＣカードが挿脱される車載機とを備え、前記ＩＣカードに移動体側暗号鍵群を示すデータが格納され、前記道路側制御装置に道路側暗号鍵群を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定することから、前記移動体側暗号鍵群は、前記車載機に代えて前記ＩＣカードに保存され、またさらに、前記移動体側暗号鍵群と同一な

11

（共通する）前記道路側暗号鍵群は、前記道路側制御システムにしか保存されておらず、前記移動体側暗号鍵群について、前記ＩＣカードを持たない第三者が知り得る可能性を最小限に抑えることができ、前記ＩＣカードの偽造を有効に防止することができる。

【図面の簡単な説明】

【図１】図１は、本発明の有料道路の料金収受装置におけるセキュリティ装置の一実施形態を示す装置ブロック図である。

【図２】図２は、本実施形態において行われる認証手続きの流れを示す図である。

【図３】図３は、一般の有料道路の料金収受装置におけるセキュリティ装置を示す装置ブロック図である。

【図４】図４は、一般の有料道路の料金収受装置におけるセキュリティ装置において行われる認証手続きの流れを示す図である。

【符号の説明】

１…ＩＣカード

２…ＣＰＵ（カード側）

３…メモリ

12

＊５…ＣＰＵ（車載機側）

７…車載機

７Ａ…移動体側制御装置（移動体側制御システム）

９…第１のアンテナ

１０…第１のアンテナコントローラ

１１…道路側第１のメモリ

１２…第２のアンテナ

１３…第２のアンテナコントローラ

１４…道路側第２のメモリ

１９…道路側コントローラ

２０…中央制御システム

２１…道路側制御装置（道路側制御システム）

Ｋ３…移動体側暗号鍵群

Ｋ４…道路側暗号鍵群

Ｒ３…第１の暗号化情報

Ｒ４…第２の暗号化情報

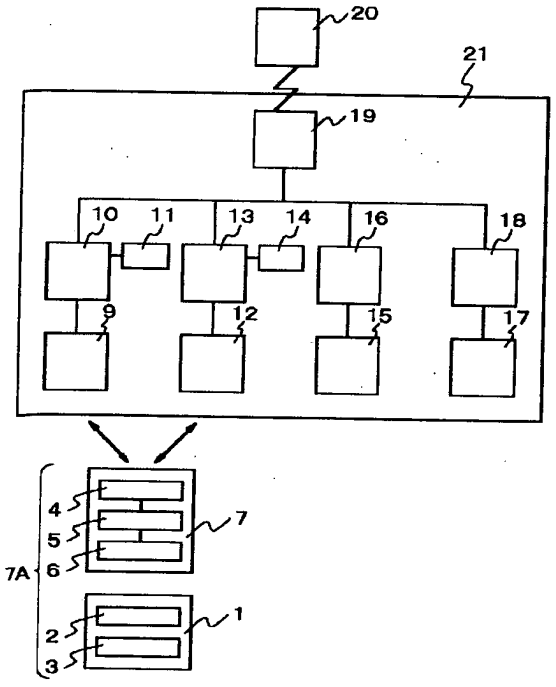
Ｓ３…第１の生成情報

Ｓ４…第２の生成情報

Ｓ５…第３の生成情報

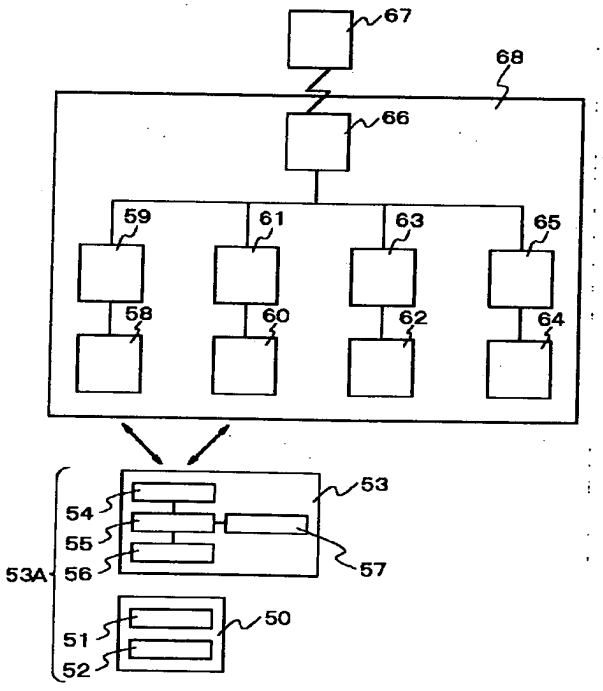
Ｓ６…第４の生成情報

【図１】



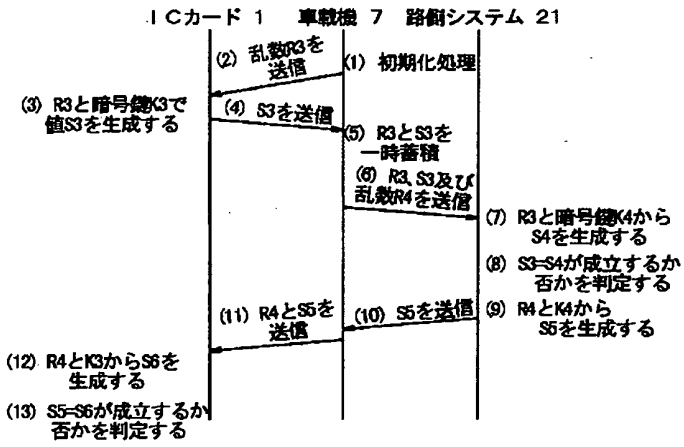
本発明の料金収受システム

【図３】

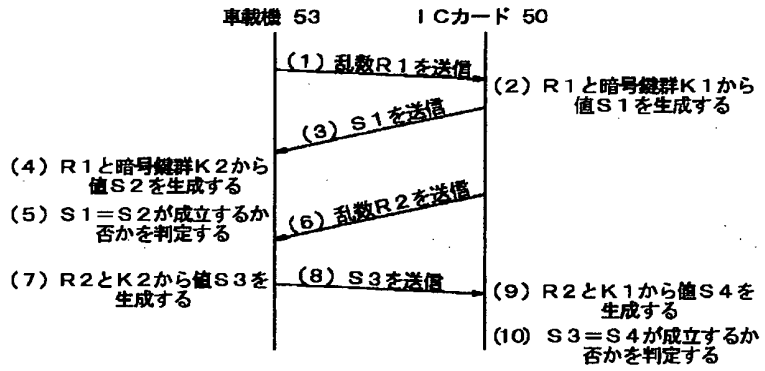


従来の料金収受システム

【図２】


ＩＣカード 1
車載機 7
路側システム 21
(2) 乱数R3を送信
(1) 初期化処理
(3) R3と暗号鍵K3で値S3を生成する
(4) S3を送信
(5) R3とS3を一時蓄積
(6) R3, S3及び乱数R4を送信
(7) R3と暗号鍵K4からS4を生成する
(8) S3=S4が成立するか否かを判定する
(11) R4とS5を送信
(10) S5を送信
(9) R4とK4からS5を生成する
(12) R4とK3からS6を生成する
(13) S5=S6が成立するか否かを判定する

【図４】


車載機 53
ＩＣカード 50
（１）乱数Ｒ１を送信
（２）Ｒ１と暗号鍵群Ｋ１から値Ｓ１を生成する
（３）Ｓ１を送信
（４）Ｒ１と暗号鍵群Ｋ２から値Ｓ２を生成する
（５）Ｓ１＝Ｓ２が成立するか否かを判定する
（６）乱数Ｒ２を送信
（７）Ｒ２とＫ２から値Ｓ３を生成する
（８）Ｓ３を送信
（９）Ｒ２とＫ１から値Ｓ４を生成する
（10）Ｓ３＝Ｓ４が成立するか否かを判定する